

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF:
The premises known as the offices of
Google Inc., 1600 Amphitheatre
Parkway, Mountain View, CA 94043
Account: aswift889@gmail.com

CR 5:20-mj-75

REDACTED
AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION

[illegible]

INTRODUCTION AND AGENT BACKGROUND

I, Brent Gromer, being duly sworn, state as follows:

1. I am a Supervisory Special Agent with the South Dakota Division of Criminal Investigation. I have been employed as a Law Enforcement Officer in the State of South Dakota for over 23 years. In 2018, I became a Task Force Officer (TFO) for the Federal Bureau of Investigation. I have been involved in numerous investigations into all manner of crime. I have received training in Search and Seizure from the South Dakota Attorney General's Office, United States Attorney's Office, the United States Drug Enforcement Administration, Federal Bureau of Investigation and other private training organizations. I have personally prepared numerous affidavits in support of request for search warrant. State and Federal courts have granted search warrants based on those affidavits that have withstood suppression efforts.

2. Since June of 2010, I have been assigned to the Internet Crimes Against Children (ICAC) Task Force in South Dakota. During that time, I have

received additional training in collecting, preserving and analyzing evidence stored in different digital formats. The following is a list of specialized training I have received in conducting digital investigations and digital forensic examinations:

- Peer-to-Peer Computer Investigations
- Access Data BootCamp
- ICAC Unit Supervisor
- Internet Forensics
- Windows 7 Forensics
- Internet Relay Chat
- MAC Forensics
- Basic Data Recovery and Acquisition
- Intermediate Data Recovery and Acquisition
- Secure Techniques for On-Scene Preview
- Identification and Seizure of Electronic Evidence
- ICAC Ares
- Child Exploitation
- ICAC eMule Investigations
- Child Pornography the Ultimate Tool to Rescue Children
- ICAC BitTorrent Investigations
- Identification of Child Sex Trafficking
- NUIX Basic
- Cybertip Management
- 2014 Techno Security Conference
- 2015 National ICAC Conference
- 2015 Crimes Against Children Conference
- Android Open Source Forensics – Epyx Forensics
- Online Ads Investigations
- Undercover Chat Investigations
- Forensics Investigations with NetClean/Griffeye Analyze
- 2016 National ICAC Conference
- 2016 State of the States Cyber Crime Conference
- 2016 Florida ICAC Symposium
- 2017 Association of State Criminal Investigative Agencies
- 2017 Sex Offender Registry Conference
- 2017 South Dakota Technology Teachers Conference
- 2017 US Attorney's Office Law Enforcement Coordinating Committee Training Seminar
- 2017 South Dakota Society for Technology in Education Conference
- Cellebrite Training

- 2018 Appointed as a Special Deputy US Marshall under the Federal Bureau of Investigation
- Co-Chair National Internet Crimes Against Child Emerging Technology Committee
- South Dakota Center for the Prevention of Child Maltreatment Advisory Board Member.
- Griffeye Analyze DI Training.

3. In addition to the training I have received, I have presented to numerous professional groups and organizations and have testified as an expert on numerous occasions in US District Court, US Magistrate Court, and South Dakota Circuit Court.

4. During my law enforcement career, I have been involved in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of 18 U.S.C. §§ 2251, 2252, and 2252A and enticement of a minor using the internet in violation of 18 U.S.C. § 2422(b). I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography and enticement of a minor using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

5. I am aware that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the production, distribution, receipt and possession of visual depictions of a minor engaging in sexually explicit conduct, using any means or facility of interstate or foreign commerce, including by computer or utilizing the internet. I am also aware that 18 U.S.C. § 2422(b) criminalizes enticement of a person under 18 to engage in unlawful sex acts utilizing the internet.

6. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals, including other law enforcement officers, interviews of persons with knowledge, my review of documents, interview reports and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, I have not withheld information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED:

7. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to a Google, Inc. account found during the investigation of an unknown subject utilizing the Target Account, which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography) and 18 U.S.C. § 2422(b), attempted enticement of a minor using the internet, and which items are more specifically described in Attachment B. The Gmail account is: aswift889@gmail.com (also referred to in this affidavit as “Target Account”).

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachments A and B:

a. “Chat,” as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Cloud-based storage service,” as used herein, refers to a publically accessible, online storage provider that collects or child

pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to access these files easily through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

f. “Computer hardware,” as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage

devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. “Computer software,” as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform

certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. A provider of “Electronic Communication Service” (“ESP”), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. “Electronic Storage Device” includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.

l. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

m. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer to access the Internet. IP

addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

n. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

o. “Network Address Translation” or “Nat” or “Natting” as used herein is a method of remapping one IP address space into another by modifying network address information while then are in transit across a traffic routing device. It became popular when the need to preserve global address space arose. One internet-routable IP address of a NAT gateway can be used for an entire private network.

p. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing

services by means of an electronic communications system.

r. “Short Message Service” (“SMS”), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send short text messages from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

s. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

t. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**BACKGROUND ON CHILD EXPLOITATION AND CHILD PORNOGRAPHY,
COMPUTERS, THE INTERNET, AND EMAIL**

9. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve many functions for persons who exploit children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.

b. Persons, who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner and then distribute the images using email, like Gmail and Yahoo! Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone.

These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People can make electronic contact to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Persons can transfer child pornography via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.

e. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail,

among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where a user utilizes online storage is, evidence of child pornography can be found on the user's computer or external media in most cases.

10. Based on my training and experience and investigation in this case, I have learned the following about Google:

a. Google offers an e-mail service that is available free to Internet users called "Gmail." Stored electronic communications, including opened and unopened e-mail for Gmail subscribers may be located on Google's computers.

b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information.

c. Subscribers can access their Gmail e-mail accounts by activating software on a device or computer, login in using unique usernames and passwords, and connecting to high-speed Internet computers called "servers" maintained and/or owned by Google. Subscribers also may be able to access their accounts from any other computer in the world through Google's web site on the Internet.

d. When a user sends any e-mail to a Gmail e-mail subscriber the email is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes it or until the stored e-mail exceeds the storage limit allowed by Google.

e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination, usually through another subscriber's e-mail provider. Copies of sent e-mail are stored on Google's servers in the same manner as received e-mail, Google retains the email until the user deletes it or exceeds the storage limit.

f. Even if the contents of the message no longer exist on the company's servers, Google may have records of when a subscriber logged into his or her account, when a message was sent or received, as well as technical routing information that law enforcement could use to determine who sent or received an e-mail.

11. From my training and experience, I am aware that Google's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer accounts and/or files for information and the content of communications pertaining to the Target Account specified herein and in Attachment A, following the procedures described herein.

PROBABLE CAUSE

12. On February 24, 2020, Special Agent Kristopher Serra, Federal Bureau of Investigation (FBI) assigned in New York state, was working in an undercover capacity on Kik Messaging Service, a social networking and private messaging service, internet application. SA Serra was in a Kik Group titled "Family fun room (No limits)." SA Serra received a private message from Kik user "Ranger_danger89," later identified as Adam Ryan Swift, Box Elder, South Dakota. The name associated with Ranger_danger89 was listed as "Adam Ryan." During the conversation via Kik Messenger, "Adam Ryan" and SA Serra's undercover persona (hereinafter "UC") discussed being "active." I know that "Active" is a chat term used to describe people who are sexually active, usually meaning with children. During the conversation, "Adam Ryan" stated that he was "active" with his 4-year-old son and 7-year-old stepson. The UC advised "Adam Ryan" they were "active" with their 9-year-old stepchild. As the conversation continued, they wrote about where each of them lived. The UC Persona advised "Adam Ryan" that he lived in New York. "Adam Ryan" stated he lived in the United States but did not immediately identify where. "Adam Ryan" asked the UC for photographs of the alleged UC persona's 9-year-old stepchild. The UC stated he had only clothed images, as he did not keep "nudes" on his phone. The UC asked "Ryan" if he had photos. "Adam Ryan" replied "Same. Clothed except one of my stepson." "Adam Ryan" then sent a photograph of himself that appeared to have been taken in a vehicle. There is a young boy visible in the back seat of the vehicle in a child restraint seat. "Adam Ryan" sent

a second photograph of a young boy taken in what appears to be a grocery store and the child is sitting in a shopping cart.

13. The conversation continued and the UC asked “Adam Ryan” if he preferred “boys or girls.” “Adam Ryan” replied “Both.” “Adam Ryan” asked the UC what he preferred. The UC informed him that he had a little girl, but had never been with a boy. “Adam Ryan” asked the UC to send photographs of the girl. The UC then sent a UC photograph of a female child. The UC had previously identified the age of the “girl” as 9 years old. After the UC complied with “Adam Ryan’s” request for photos of his 9-year-old step- daughter, “Adam Ryan” replied “Yummy, I love them younger than that!” “Adam Ryan” asked the UC what he had done with the girl. The UC responded, in a manner implying the UC had engaged in sexual penetration with the child. The UC asked “Adam Ryan”, “You got any vids?” “Adam Ryan” initially responded that he did not have any of him. The UC then asked for “anything young?” Ryan then sent a video titled:

Bdd7beac-af8a-4cef-82a3-67e1052ad1f4.mp4 – This is a 1:49 video of an adult male and a female child who appears to be approximately 10-12 years of age. When the video begins the child is lying on her left side and the male is positioned near her buttocks on his knees. The male is masturbating. 6 seconds into the video the video scene changes and the child is seen on her back with her legs spread and the adult male is vaginally raping her with his penis. The rape continues through 1:15 in the video when the scene again changes to the male masturbating and ejaculating on the child’s face.

14. Thereafter, the UC commented about the high-heeled shoes the girl wore in the video. The UC then asked “Adam Ryan” where in the United States he was located. “Adam Ryan” sent a second video titled:

933552a1-21f8-4b0b-b502-f13b3390aada.mp4 – This is a 36 second video of a female child who appears to be approximately 5-7 years of age. The video shows the female child being orally raped by an adult penis. This continues to 32 seconds into the video when the camera pans to the child’s buttocks.

15. After sending the two videos, “Adam Ryan” responded to the UC’s question asking where he lived in the United States. “Adam Ryan” replied “South Dakota.” The conversation continued and the UC asked “Adam Ryan” “Whats (sic) your youngest.” “Adam Ryan” replied, “My son was 2 when I sucked him. I ate out a newborn girl fairly often. I babysat her for about a year. Licked her pussy all the time.” The conversation continued and “Adam Ryan” and the UC discussed whether their wives knew of what they were doing and both stated their wives did not know. The conversation concluded on February 24, 2020.

16. SA Serra prepared a report and sent that to SA Erik Doell, FBI Rapid City. SA Doell contacted me and asked if the SD ICAC Task Force would conduct the follow up investigation. SA Doell provided me the report prepared by SA Serrra and the results of SA Serra’s investigation. SA Serra had prepared a subpoena for the IP addresses used to access Kik Messaging Service from February 11, 2020, through February 24, 2020. Kik Messaging service provided a list of IP Addresses. The user accessing the Ranger_danger89 account was

accessing Kik Messenger through IP Address 24.111.189.122, which Midcontinent Communication owns. SA Serra had sent a subpoena to Midcontinent for the subscriber information for the lessee of this IP Address on February 24, 2020. Midcontinent responded that the lessee of the IP Address was Fox Den Store-It, located at 12192 Siouxland Rd., Summerset, SD.

17. In addition to the IP information, Kik Messenger identified aswift889@gmail.com (SUBJECT ACCOUNT) as the email address associated with the Ranger_danger89 account.

18. I conducted a search of local records for Adam Swift based on the information received from Kik Messenger and Midcontinent Communication. I located local resident:

Adam Ryan Swift

[REDACTED]

DOB: [REDACTED] 89

19. I conducted a search of Facebook.com and located a publicly accessible page belonging to Adam Swift. In review of the information listed on Adam Swift's Facebook page, I learned that Adam Swift listed he was a sales manager for Fox Den Store-it in Summerset, SD, the same location where "Adam Ryan" accessed the Ranger_Danger89 Kik Messenger account. Through further examination of the information provided by SA Serra and the information on Swift's Facebook page, I located the same photograph in Facebook as was used for the Kik Messenger profile photograph for Ranger_danger89.

20. I then contacted United States Homeland Security Investigations Special Agent Scott Beagle. SA Beagle commonly works on line in an undercover

capacity. I asked SA Beagle to offer Swift the opportunity to communicate with him via Kik Messaging Service. SA Beagle introduced himself to Swift, via the Ranger_danger89 Kik user account on March 10, 2020, writing, “24f.26m.5yo.active fam here”, meaning, the “family” was made up of a 24-year-old female, a 26-year-old male and a 5-year-old child who were “active” as described above. Swift thereafter responded. During the conversation, SA Beagle portrayed himself as a 24-year-old female with a 5-year-old daughter. Swift informed SA Beagle’s UC Persona that he was engaged to be married and had two children, ages 4 and 6. During the conversation SA Beagle and Swift exchanged photographs. The photograph provided by Swift again matched the previously described photographic identification. SA Beagle asked Swift, “So what r u into? Looking for?” Swift replied “Into anything no limits. Looking for other taboo families and ideally one that would let me use their daughter one day.” SA Beagle’s UC persona stated they have let “outsiders in for our daughter” and reminded him the “daughter” was 5 years old. Swift replied, “I love it” then added, “The youngest I’ve had was 3.” SA Beagle’s persona asked about Swift’s experience. Swift wrote, “Friends (sic) kid and being raised that way.” A couple of messages later SA Beagle’s persona asked Swift if he was “active” and if he was serious about meeting with the UC persona’s daughter. Swift replied, “Yes I’m serious and active”. SA Beagle’s persona asked Swift with whom he was “active”. Swift wrote he was “active” with his son and later added, “I suck him”. Swift and SA Beagle’s persona wrote about how long each of them had been “active” and how they had begun in the “lifestyle”. As the conversation

continued, SA Beagle's persona asked Swift what Swift wanted to do with the UC's "daughter". Swift replied, "I'd love to eat her out and fuck her pussy". SA Beagle's persona again reminded Swift the child was only 5 years old and not allowed to engage in penetration. Swift then wrote, "I'll eat her out as much as I can". Swift asked SA Beagle's persona, "So you don't want to do anything with my son?" Swift told SA Beagle's persona that she could do "anything you want", and added "I want to watch you suck him". Swift and the UC wrote about whether their significant others knew about the abuse with the children. Swift advised his fiancé did not know he was abusing his son. As the conversation continued, Swift asked the UC for photographs of the child. At Swift's prompting, they also discussed arranging a time to meet and "swap" the children. They talked about a workable schedule for the meeting. They set Friday, March 20, 2020, as the potential for an initial meeting date.

21. Swift continued to write about what the child would like. He asked the UC, "She enjoy being ate out?" When the UC replied, "Yes". Swift wrote, "Good! I want her sitting on my face". Swift asked the UC if he would allow "gentle fingering" of the girl. Swift went on and asked the UC "She suck (sic) cock yet?"

22. The conversation continued and the UC and Swift further discussed being in the "lifestyle". Swift informed the UC, "I was used by my dad and brother and was allowed to eat my sister out but never allowed to fuck her." The conversation continued and the UC mentioned a Kik group to which he belonged and Swift asked if he wanted to join. When Swift answered affirmatively, the UC

stated Swift could, but that Swift would have to “verify.” I know that “verify” means to send a proof-of-life-type video to show the person is not law enforcement. Swift agreed and sent a video of himself to the UC. In the video, Swift was in a car talking to the camera and stated, among other things that, “Today is March 10th”.

23. During the conversation, Swift and the UC also wrote about what each other did for jobs. Swift informed the UC that he was a Manager at Fox Den Store-it. Swift asked the UC several questions about “her and her husband” and “the lifestyle”. Swift told the UC, “I think you’ll love sucking on my son. He loves having it done!” He told the UC, “He likes to moan and place his hand on my head while I do it”. When the UC questioned him about the veracity of this statement, Swift explained, “It’s just an orgasmic moan. It’s just a simple moan”. Swift asked the UC if “she” wanted him to “prove it”. The UC discouraged Swift from proving he was sexually abusing his son. The conversation on March 10, 2020, concluded shortly after.

24. The UC Persona talked about possible meeting dates with Swift, however Swift wrote that he was going to be out of state in Wisconsin until Saturday, March 14, 2020. SA Beagle monitored the Ranger_Danger89 account, but found that Swift had not accessed the account until March 19, 2020, when the conversation continued.

25. On March 19, 2020, SA Beagle received additional messages from Swift via Kik Messenger. Swift told the UC that he had just gotten back and asked the UC “how’s your princess”. The UC asked Swift if it still worked to meet

on March 20, 2020. Swift replied, "To show you video and pics?" The UC then wrote that he meant for the previously discussed meeting on March 20, 2020. Swift then said he could not meet on March 20, 2020 because he had to work until 8 pm. He said he would be available to meet over the weekend of March 21, 2020 and March 22, 2020. The UC asked Swift what he meant by sending pics and vids". Swift explained, "I can send you pictures and videos of my son while I play with him". Again, the UC discouraged Swift from doing that. Swift added that he would be off on Wednesday, March 25, 2020, and would be available to meet then. Swift informed the UC that he would create live videos while he abused his son or would do a live chat while he abused his son. The UC corrected him about dates available for meeting and Swift wrote that he liked a woman who "took charge". The UC informed him that she was not into him. Swift replied, "I know that", "And you aren't really my type, I just like when women take charge". Swift then told the UC, "I can't wait to taste your princess's pussy". The UC suggested when they met for the first time, that Swift leave his son at home and Swift could just meet with the UC's daughter. Swift wrote "Yeah? I'd love that!", and added "Have you watch me use her as my own little fuck toy", "Think she would enjoy my tongue?" and added "I'd love to feel her tight pussy on a finger too". The UC Persona asked Swift if he would be able to meet right away. Swift said he wished that he could, but indicated he was currently working.

26. When the UC confronted Swift that the communications were just "fantasy," Swift replied, "I'm serious!" and added "I'm very horny and hard for

her right now.” The UC again reminded Swift she was only 5. They then agreed that Swift would contact the UC at approximately 5:00 pm Mountain time on March 19, 2020 to inform whether he was available to meet that night. When Swift replied he said he was not available that night and set a plan to meet either that weekend or the following Wednesday.

27. The same day, Homeland Security Resident Agent in Charge (RAC) Nick Saroff, conducted surveillance in the area of Fox Den Store-It in Summerset, SD, the location of which the IP address to the Ranger_danger89 Kik account returned. He was not able to confirm that Swift was at the business as he said that he would. SA Michelle Pohlen, HSI, conducted surveillance in the area of Swift’s residence. She was not able to locate Swift’s vehicle at that time. She did verify the property information set forth above and obtained the photographic warrant attachments. On March 12, 2020, SA Pohlen also surveilled Swift’s apartment complex and located his vehicle, a gray Ford Fusion bearing SD Veteran’s Lic.: 0973G. On March 19, 2020, SA Pohlen checked the area of Fox Den Store-It at 2810 Eglin St., Rapid City. She located Swift’s gray Ford Fusion and she was able to see Swift inside of the business as she conducted surveillance.

28. On Monday, March 23, 2020, Swift inquired of the UC, “What all do you want me to do with her on Wednesday?” The UC responded, “U tell me. Honestly we dont (sic) care. Been a brat lately”. Swift asked, “Yeah? How so?” The UC replied, “Just 5yo stuff. Anyway.” Swift then wrote, “Oh, ok” and added, “I’d love to start by bathing her and stroking her young pussy lips in the

bathwater. Then after she is all dry, have mommy and daddy hold her hands and legs while I taste her. Once I get her pussy nice and swollen, i (sic) will finger fuck her good and deep.” The UC replied, “Were good with that.” Swift then added, “Good! Where am I allowed to cum? I know not in her pussy, but can I make her open her mouth for it, or cum on her face, or cum on her pussy?” The UC said they would discuss specifics on Wednesday. The UC then inquired about Swift’s son. Swift then wrote, not in response to the UC’s question, “Where do you want to meet first? Or just want me to show up at your house?” Then he responded regarding his son writing, “He is good. He missed me.”

29. The UC then commented on it being good to find “like minded” people and Swift agreed. The UC then asked about the “groups” Swift was in and Swift responded, that he was not in any others and “The rest were full of weirdos with no ACTUAL experience.” He added, “There was one that I was in where everyone was trading some really sexy pictures. But none of them were of actual people they knew” and that “real people are more exciting.” Swift then admitted to trying to meet a woman in the past to “have” her three daughters under 7 but the woman moved away before that could occur.

30. Swift informed the UC, “One of my biggest desires is to have a multifamily home where anyone’s kids and spouses are fair game for play.” Swift then assured the UC they would meet “tomorrow,” the 25th, and again he asked where they would meet. Swift later asked for a picture of the UC and her “hubby” and the UC refused. They then discussed the need for secrecy regarding Swift’s abuse of the UC’s daughter and he added, “I wouldnt (sic) want it getting around

what you will do with my son.” Swift then wrote, “Have play dates for the kids as often as possible,” and “I’m excited to watch you explore his body and play with him and let him taste you,” and “it will be a great experience.” Swift then sent the UC a picture of a young boy, smiling at the camera. After that, Swift wrote, “I honestly do want this to become a regular thing with the 5 of us!”

31. Swift then wrote of his concerns that his soon-to-be victim would be “uncomfortable” and “nervous.” The UC informed Swift that the girl would like it if he brought her a coloring book or lip-gloss. The UC further encouraged Swift to bring her those items because they “were not charging” him for sex with the girl.

32. When the UC asked Swift what he wanted the UC to do with Swift’s son, Swift responded, “I want to watch you such on his dick and teach him to lick your pussy. If you wanted to try to get him to slide into you, that would be a bonus. But whatever you’re comfortable with!” Swift then informed the UC he would help “slide it in” and that he would “hold it up” with his “fingers” and she could “sit down on it.” And, “I’d love to see how he reacts to tasting your pussy. I think he would love it.” Swift then suggested that the two children engage in sex acts with one another. After asking whether the UC’s “daddy” tried to get the child to “suck him,” Swift added, “Then I’d like her to do that to me and to [REDACTED].” [REDACTED] is his son’s name. The UC then verified that Swift was not bringing his son to the March 25 meeting and Swift agreed it would be “just us 4” and sent a picture of himself in front of storage lockers. Swift then admitted

that he had been, “turned on and hard all morning knowing how close its getting.”

33. Later in the communications, Swift said he intended to sexually abuse his 4-year-old son tonight (March 24, 2020). Based on that, law enforcement decided to change plans from meeting on March 25, 2020, to March 24, 2020, to avoid the opportunity for him to abuse his son. The UC asked if Swift would be willing to meet with her husband in order to put their minds at ease and to set up the specifics of the sexual encounter on the 25th. The UC offered that her husband go to Swift’s location of employment to achieve the meeting, Swift agreed and provided his work’s location information, the Fox Den Store-It on Moon Meadows Rd. in Rapid City. They agreed that the UC’s husband would pull up out front and Swift would leave his work and meet in order for the UC’s husband to make sure the situation was legitimate and to provide Swift with the address he would go to the following day to sexually abuse the 5-year-old girl. Swift informed the UC he had a meeting until 4:45pm.

34. Several law enforcement officers surveilled that location and verified Swift’s car was there. Swift sent a message to the UC saying his meeting was over and the UC’s husband could go to meet him. Utilizing another local UC agent, law enforcement proceeded to Swift’s work. Beagle continued to communicate with Swift and informed Swift of the vehicle description the local UC was driving.

35. Just before 5pm, the local UC pulled into the parking lot of the Fox Den Store-It and Swift immediately left the office, walked to the passenger side

of the vehicle and got in. After a brief discussion, Swift told the UC he needed to assist a customer in exiting the gated area of the storage unit, got out of the UC vehicle, walked toward the gate, assisted the customer and got back into the UC vehicle. The UC then mentioned to Swift that he was there to give Swift the address and Swift mentioned being anxious for the meeting. At that point, I had law enforcement arrest Swift.

36. Swift consented to seizure of his cell phone, laptop computer and the black and red computer storage backpack (SUBJECT ITEM) in the office.

37. Swift agreed to an interview with me. He admitted it was he communicating with the UC, but claimed that it was just about the sexual dialogue and that he would not have engaged in sex with the minor. He also denied sexually abusing his 4-year-old son. Swift also consented to a polygraph. The polygraph resulted in Deception Indicated, meaning that Swift failed the polygraph examination. In the post-polygraph interview, he admitted that when he was 18 years of age he engaged in a sexual relationship with a girl that may have been 15 years of age at the time. Swift further admitted that his son had touched his (Swift's) penis on two occasions. Swift stated his family are "in home nudists" and he was setting next to his son, when Swift's son (4 year old, [REDACTED]) reached over and touched the base of Swift's penis. Swift indicated he had told his son, that he had his own penis and should not touch others. Swift continued and admitted that Swift had touched [REDACTED]'s penis on one occasion in the bathtub. Swift stated this occurred approximately 2 years prior to 3/24/20. Swift said he was bathing [REDACTED] and [REDACTED] got an erection. Swift said that he

touched the base of [REDACTED]'s penis out of curiosity and described this touch as a prolonged touch.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL
INTEREST IN CHILDREN AND/OR WHO RECEIVE AND/OR POSSESS
CHILD PORNOGRAPHY**

38. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to

seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. The user often maintains these child pornography images for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy

correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time-period. Law enforcement officers involved in the investigation of child pornography throughout the world have documented this behavior. Thus, even if the unknown user uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found within the SUBJECT ACCOUNT.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

40. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a “district court of the United States (including a magistrate judge of such court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

41. The United States respectfully applies for an order of nondisclosure to Google, Inc. under 18 U.S.C. § 2705(b) regarding the following account: aswift889@gmail.com. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding Google, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or

modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to Google, Inc., persons can modify its content with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Google, Inc. not to notify the user of the existence of this warrant.

LIMIT ON SCOPE OF SEARCH

42. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

43. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by Google, Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the Google, Inc. account, listed in Attachment A has been used for the exploitation of children using the internet including violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography), which items are more specifically described in Attachment B. There is probable cause to believe that the unidentified user of the Gmail account received child pornography and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere. The account is the subject of this

warrant affidavit. The account is: aswift889@gmail.com.

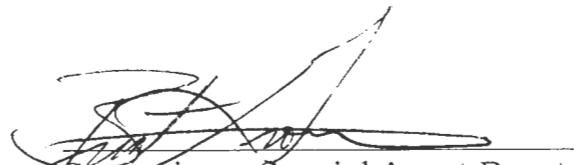
44. Law Enforcement agents will serve the warrant on Google, Inc., who will then compile the requested records at a time convenient to it, so there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

45. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of federal criminal law. Additionally, I request authority to serve the warrant on Google, Inc. via the internet and to allow Google, Inc. to copy the data outside of this agent's presence.

RETURN COMPLIANCE BY GOOGLE, INC.

46. Google's policies prohibit mailing or emailing child pornography to law enforcement in response to a search warrant, instead requiring a law enforcement officer to personally appear and collect contraband materials, unless the means of production is explicitly described in that search warrant. Specifically, Google requires the Court order the disclosure, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

Further your affiant saith not.




Supervisory Special Agent Brent
Gromer, SD DCI and SD ICAC
Commander, FBI TFO

SUBSCRIBED and SWORN to

_____ in my presence

X by reliable electronic means

this 1st day of April, 2020.



DANETA WOLLMANN
U.S. MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with the following Gmail email account, under an account known to be stored at the premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043: aswift889@gmail.com

ATTACHMENT B
**Particular Things to be Seized and Procedures
to Facilitate Execution of the Warrant**

I. Information to be disclosed by Google, Inc. (the “Provider”) to facilitate execution of the warrant:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google Inc., including any emails, records, files, logs, or information that have been deleted but are still available to Google Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on March 17, 2020. Google Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, including any information contained in the email account which is helpful to determine the accounts’ user’s or owner’s true identity:

a. The contents of all e-mails associated with the account, from the time of the account’s creation to the present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each e-mail;

b. The contents of all Instant Messages (IM) associated with the account, from the time of account’s creation to the present, including stored or preserved copies of IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP addresses used to register the account, all log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of services utilized;

e. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between Google Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that was created or saved after the creation of the account that is the subject of this warrant and that constitutes contraband or fruits, evidence or instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, (production, receipt and possession of child pornography) including, for the account or identifiers listed on Attachment A, information pertaining to the following matters:

- a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, or attempting or conspiring to do so;
- b. Any person knowingly distributing, receiving, or possessing child pornography as defined at 18 U.S.C. § 2256(8), or attempting or conspiring to do so;
- c. Any person knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged, or attempting to do so;
- d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the email account owner or user;

- e. Evidence indicating the email account users or owner's state of mind as it relates to the crime under investigation;
- f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
- g. Records relating to who created, used, or communicated with the electronic account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card information and money wire transmittal information, including bills, payment records, and any receipts, for payments to third party money remitters, including Xoom.com, Western Union, PayPal, and MoneyGram.

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A, including evidence of their whereabouts;

4. Evidence of the times the user utilized the account or identifiers listed on Attachment A;

5. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifier listed on Attachment A and other associated accounts.

III. Information Regarding Search Warrant Compliance by Google:

Google shall disclose responsive data, if any, by sending to:

Special Agent Brent Gromer
____ Fountain Springs Plaza
Rapid City, SD 57702
605-381-1734
Brent.Gromer@state.sd.us

Google shall use the United States Postal Service or another courier service to disclose the responsive data, notwithstanding 18 U.S.C. § 2252A or similar statute or code. In the alternative, Google may make the responsive data available to Special Agent Gromer by use of its law enforcement portal.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL
RULE OF EVIDENCE 902(11) and (13)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google Inc., and my official title is _____.

I am a custodian of records for Google Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google Inc.; and

c. such records were made by Google Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature